Beletten dat radiofrequenties van draadloze RADIUS-netwerkmodules op grote schaal

Inhoud

Inleiding

Dit document biedt een kort overzicht van de basisconfiguratiehandleidingen voor draadloze implementaties op grote schaal zoals de AireOS Wireless LAN Controller (WLC) met RADIUS en Cisco Identity Services Engine (ISE) of de Cisco Secure Access Control Server (ACS). Dit document verwijst naar andere documenten met meer technische details.

Symptomen waargenomen

Meestal worden universiteitsomgevingen geconfronteerd met deze staat van verificatie, autorisatie en accounting (AAA). In dit gedeelte worden de gebruikelijke Symptomen/Logs beschreven die in deze omgeving zijn waargenomen.

1. Controleer RADIUS-prestaties

De Dotx Client ervaart een grote vertraging met veel pogingen om authentiek te verklaren.

Gebruik de opdracht **Straalautestatistieken tonen** (GUI: **Monitor > Statistieken > RADIUS servers**) om naar problemen te zoeken. Meer in het bijzonder, zoek grote aantallen Retries, Afwijzingen en Time outs. Hierna volgt een voorbeeld:

```
Server Index..................................... 2
Server Address................................... 192.168.88.1
Msg Round Trip Time.............................. 3 (msec)
First Requests................................... 1256
Retry Requests................................... 5688
Accept Responses................................. 22
Reject Responses................................. 1
```

```
Challenge Responses..... 96
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 1
Timeout Requests..... 6824
Unknowntype Msgs..... 0
Other Drops..... 0
```

Zoek naar:

- Snel opnieuw proberen: Verhouding eerste aanvraag (mag niet meer dan 10% zijn)
- Hoog afwijzen: Acceptatie-verhouding
- High Time-out: Eerste aanvraag ratio (mag niet meer dan 5% zijn)

Als er problemen zijn, controleert u op:

- Misleide klanten
- Problemen met netwerkbereikbaarheid tussen de WLC en de RADIUS-server
- Problemen tussen de RADIUS-server en de backend-database, indien gebruikt, zoals met Active Directory (AD)

2. In het WLC wordt de RADIUS-wachtrij op de MGBT-bestanden geplaatst

WLC ontvangt dit bericht over de RADIUS-wachtrij:

```
Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.
```

3. Debug AAA

Dit bericht is te zien op een debug van AAA:

```
*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx
```

Een debug van AAA retourneert de AAA fout **timeout (-5)** voor mobiele apparaten. De AAA-server is onbereikbaar en wordt gevolgd door een vergunning van de klant.

4. RADIUS-server is te druk en reageert niet

Hier is de logsysteemtijdtrap:

```
0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
```

```
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
```

Best Practice Tuning

WLC-zijtuning

- Extensible Authentication Protocol (EAP) - Maak de uitsluiting van 802.1X-clients mogelijk.

  Schakel uitsluiting van klanten wereldwijd in voor 802.1X.
  Stel clientuitsluiting op de 802.1X draadloze LAN's (WLAN's) in op ten minste 120 seconden.
  Stel EAP-timers in zoals beschreven in de 802.1X clientuitsluiting op een AireOS WLC-artikel.

- Stel de RADIUS-retransmissietijden in op ten minste vijf seconden.

- Stel de sessie-tijd in op ten minste acht uur.

- Schakel Aggressief failover uit, waardoor geen enkele fout-gedraging mogelijk is waardoor de WLC tussen de RADIUS-servers defect raakt.

- Configureer snel beveiligde roaming voor uw klanten.

  Zorg ervoor dat Microsoft Windows EAP-klanten Wi-Fi Protected Access 2 (WAP2)/Advanced Encryption Standard (AES) gebruiken zodat ze opportunistische Key Caching (OKC) kunnen gebruiken.

  Als u Apple iOS-clients kunt segregeren naar hun eigen WLAN, kunt u 802.11r op die WLAN inschakelen.

  Cisco Centralised Key Management (CCKM) inschakelen voor elke WLAN die 792x-telefoons ondersteunt (maar geen CCKM inschakelen op elke Service Set-id (SSID) die Microsoft Windows of Android-clients ondersteunt, omdat ze vaak problematische CCKM-implementaties hebben).

Schakel Sticky Key Caching (SKC) in voor elke EAP-WLAN dat de Macintosh Operating System (MAC OS) X en/of Android-clients ondersteunt.

Raadpleeg 802.11 WLAN-roaming en Fast-Secure roaming op CUWN voor meer informatie.

Opmerking: Bezoek uw geheugen (WLC Pairwise Master Key, PMK) op piektijden met de **show pmk-cache alle** opdracht. Als je de maximale PMK-cache grootte bereikt, of dicht bij hem komt, dan moet je waarschijnlijk SKC uitschakelen.
Als u ISE met profilering gebruikt, gebruik dan DHCP/HTTP-profilering aan de WLC-zijde. Dit verpakt de profilerende gegevens in een pakket van de Rekening van de RADIUS dat makkelijk load-evenwichtig is, dat ervoor zorgt dat alle gegevens voor het eindpunt het zelfde Netwerk van de Openbare services (PSN) bereiken.

Zorg ervoor dat tussentijdse accounting niet mogelijk is tenzij u deze nodig hebt voor byte-gebaseerde factureringsservices. Anders voegt een tussentijdse accounting alleen lading toe zonder extra voordeel.

Start de beste WLC-code.

RADIUS-serverzijtuning Verlaag de houtkapsnelheid. De meeste RADIUS-servers zijn Configureerbaar over wat ze zullen opslaan. Als ACS of ISE wordt gebruikt, kan een beheerder kiezen welke categorieën aan de controlegegevensbank worden geregistreerd. Een voorbeeld kan zijn als de boekhoudgegevens van de server van de RADIUS worden verzonden en met een andere toepassing zoals SYSLOG worden bekeken, dan de gegevens niet lokaal naar de database schrijven. Zorg er op ISE voor dat de logsuppressie altijd ingeschakeld blijft. Als het moet worden uitgeschakeld voor de oplossing van problemen, ga dan naar **Beheer > Systeem > Vastlegging > Verzamelfilters** en gebruik de optie Bypass Suppression om onderdrukking op een individueel eindpunt of gebruiker uit te schakelen. In ISE Versie 1.3 en hoger kan een eindpunt met de rechtermuisknop geklikt worden in het logboek van de bewegende authenticatie om ook suppressie uit te schakelen.

Zorg ervoor dat de authenticatielatentie aan de achterkant laag is (AD, Lichtgewicht Directory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Als u de ACS of de ISE gebruikt, kunnen de authenticatie summiere rapporten worden uitgevoerd om de latentie per server te controleren voor zowel gemiddelde als piekvertraging. Hoe langer het duurt voordat een verzoek wordt verwerkt, hoe lager de authenticatiegraad van het ACS of de ISE kan worden verwerkt. 95% van de tijd, hoge latentie is te wijten aan een trage respons van een backend database.

Schakel de PEAP-wachtwoordherhalingen (Protected Extensible Verification Protocol) uit. De

meeste apparaten ondersteunen geen wachtwoordherhalingen in de PEAP-tunnel, dus als de MAP-server opnieuw probeert, kan het apparaat niet meer reageren en opnieuw beginnen met een nieuwe MAP-sessie. Dit veroorzaakt EAP-onderbrekingen in plaats van afwijzende opmerkingen, wat betekent dat de uitsluiting van klanten niet zal worden doorkruist.

Ongebruikte EAP-protocollen uitschakelen. Dit is niet van cruciaal belang, maar draagt wel bij aan de efficiëntie van de MAP-beurs en zorgt ervoor dat een cliënt geen gebruik kan maken van een zwakke of onbedoelde MAP-methode.

PPPoE-sessie inschakelen en snel opnieuw aansluiten.

Verzend geen MAC-verificatie naar de AD indien niet nodig. Dit is een veel voorkomende misconfiguratie die de lading op de domein controllers verhoogt waartegen ISE authenticeert. Deze leiden vaak tot negatieve zoekopdrachten die tijdrovend zijn en de gemiddelde latentie vergroten.

Gebruik de apparaatsensor (indien van toepassing) (ISE-specifiek).